Division of Information Technology Services
Department of Administrative Services
State of Utah

September 16, 2002

Operational Acceptance Testing Policy for Network Centric Applications

Policy Objective and Scope: This policy describes the guidelines for operational acceptance and testing for network centric applications. Strict adherence to this policy is necessary in order to preserve the integrity of the State WAN and thus guarantee that all executive branch agencies can rely on their data communications. This policy is intended to be a point of reference for developers and vendors wishing to propose solutions that will in any way effect the State Network.

Definitions
Production Network Environment: refers to the network environment that receives IP services from the State owned IP blocks and routes or switches this traffic.

Well-Known Exploits: Because of the dynamic nature of security, defining "well-known exploits" would be almost impossible to keep up with. For the purposes of this document, we will defer to the judgment of the State Security Team to keep a list of well-known exploits available and rely on them keeping that list as current as possible.

Introduction and Rationale
State executive branch agencies and rural area customers save literally hundreds of thousands of dollars each year due to their combined financial support of ITS in the area of data communications. The task of maintaining this network includes securing lower carrier rates, increasing reliability and survivability, providing required bandwidth to customers, incorporating security measures for statutory mandates (CJIS, HIPAA, IRS), and preparing for new technologies such as Voice Over IP (VOIP). This policy was developed to ensure that this combined network continues to save taxpayer dollars and provide agency required service levels and functionality for all participants and technologies.

Notwithstanding cost containment considerations, agencies will have the option of paying for additional network bandwidth requirements beyond the base lined basic WAN services provided by the State, should it be deemed in the agencies and the State's interest to do so. ITS will provide full cooperation and support to meet these special requirements at least cost to the State of Utah.

Governing Team and Guidelines
A multi-agency governing team comprised of cross-functional participants, *henceforth known as the Operations Acceptance Team (OAT)*, will set product / service criteria and update all associated standards and guidelines no less than twice a year. This governing team will be comprised of employees from the executive branch agencies and will meet monthly to discuss any problems that need to be resolved.

Detailed instructions and descriptions of the criteria can be found in a document set titled, "*Operational Acceptance Plan and Test Design:"* and will include subheadings to denote the specific area of impact. When approved, these documents will be available on the State of Utah Innerweb site.

If a product / service fails to meet both the general checklist below and the product / service specific criteria set forth in the "Operations Acceptance Plan and Test Design:" documentation, then the OAT will not allow the product / service to proceed into the production network environment. Resubmission of the product / service to the team for testing will be required once all of the outstanding issues have been addressed and the product / service is ready for reconsideration by the OAT.

ITS to provide a Testing Environment
The OAT will design an environment that will be available for all agencies to use when testing applications. The diagrams and details of this environment will be made available for other departments to see and duplicate if they so desire.

General Acceptance Criteria and Checklist
The following operations acceptance checklist must be completed, as well as any required support, security and testing plans / attachments submitted, in order for the product / service to be deployed into production and begin placing traffic on the wide area network (WAN).

Testing in a controlled environment: *Additional criteria may be added when Standards are developed as outlined under the "Governing Team and Guidelines" listed above.*

(Environment to be determined by the OAT including baseline environment, traffic generation, security requirements, and any other criteria which will be relevant to maintaining the open nature of the State WAN.)

The application must undergo a network traffic analysis study including:

- ❑ A minimum graphing of bandwidth, CPU, and memory utilization statistics for all Layer 3 devices in the environment determined by the OAT. Baseline verses application implementation.
- ❑ Identification of any application specific needs (ie. timing, protocol, ports, etc.)
- ❑ Security needs beyond those defined in the "Security Compliance" section listed below.
- ❑ A list of potential locations and the numbers of users at each location around the State.
- ❑ Network fault testing has occurred where OAT defined failure scenarios are introduced and the behavior of the application is monitored and test results shared with OAT.

Points of Contact: *Additional criteria may be added when Standards are developed as outlined under the "Governing Team and Guidelines" listed above.*

- ❑ All applicable vendor points of contacts are identified and documented.
- ❑ All application authors are documented and contact information is published.
- ❑ All interface agreements / escalation procedures are agreed upon and in place.

Security Compliance: *Additional criteria may be added when Standards are developed as outlined under the "Governing Team and Guidelines" listed above.*

- ❑ The application complies with the State Information Security policy and any related or referenced policy documents. Due to the changing nature of Security, the OAT will be responsible for creating and amending "*Operational Acceptance Plan and Test Design:"* guidelines to reflect the latest in Security.
- ❑ The security of the application has been evaluated and recommendations from the State Security Team have been implemented. This may include creation of a firewall policy, VPN solution, or integration of a separate application.
- ❑ Secured access to the application has been established using approved methods (i.e. SSL, SSH, VPN).

- ❑ Authentication of users will be accomplished by the use of an LDAP compliant database. The State NDS directory and/or the Novell's Enterprise Directory Services (eNDS) as well as SiteMinder will be a future requirement and all applications will be engineered to integrate with these products. Exceptions must be approved in writing by the Chief Information Officer (CIO).
- ❑ The application has been tested, and certified, as not being susceptible to well-known exploits either through the use of common tools or published exploit code. (See the definitions "well-known exploits".)

Scheduling: *Additional criteria may be added when Standards are developed as outlined under the "Governing Team and Guidelines" listed above.*

- ❑ All release / change dates and times have been communicated to individuals and teams impacted.
- ❑ Change Management has been informed of the pending change / release, and has given approval.

Prior to a Total State Wide release: *Additional criteria may be added when Standards are developed as outlined under the "Governing Team and Guidelines" listed above.*

- ❑ Three locations (State WAN sites with combined agency presence) will be identified as test sites and baseline statistics will be saved. These baselines will include Hub, Geographic Hub, and Data Center statistics.
- ❑ The application will be deployed and testing of the application will begin.
- ❑ The impact on other services and applications, as well as overall network performance will be documented. Performance and test results will then be published and any impacted parties will be made aware of any foreseeable problems.

Monitoring ability: *Additional criteria may be added when Standards are developed as outlined under the "Governing Team and Guidelines" listed above.*

- ❑ All applications will have monitoring abilities made available to ITS. (SNMP type polling of individual application(s) / service(s).) This will be for the purposes of providing application availability to departments as part of ongoing customer service levels.

Vendors Information

This policy will be a requirement of current and future RFP's and bids used supported or drafted by state agencies to purchase services that may impact the State Network. All contracted vendors shall strictly adhere to these standards as a part of the development process of any application(s) for agencies and customers participating in the State WAN.

References:

Interim Date: Pending
Organization Sponsoring the Standard: ITS, and the CIO
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: June 27, 2002 (Draft Presentation) and presented for approval on September 26, 2002.
Author(s): David Lee, Wade Billings, Rick Gee, John Stucki, John Malouf and Robert Woolley (ITS)
Related Documents: Governor's Executive Order of December 11, 2001**,** State Information Security Charter, State Network Access Policy, State Information Security Policy, Operational Acceptance Plan and Test Design.